REMARKS

Favorable reconsideration and allowance of the claims of the present application are respectfully submitted.

In the present office action, constituting a Final Rejection, Claims 1-4, 12 and 14 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Brennan et al. (U.S. Patent No. 5,675,649) (hereafter "Brennan") in view of Arditti et al. (U.S. Patent No. 6,125,445) (hereafter "Arditti"). Moreover, Claims 5 and 16 were rejected finally under 35 U.S.C. § 103(a) as allegedly being unpatentable over Brennan in view of Boudot (Eurocrypt 200, LNCS 1807, pp. 431-444, 200) (hereafter "Boudot"). Furthermore, Claim 6 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Brennan in view of Boudot as applied to Claim 5 above, and in further view of Matyas et al. (U.S. Patent No. 5,265,164) (hereafter "Matyas"). In addition, Claims 7, 10, and 18, stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Chaum (U.S. Patent No. 4,996,711) (hereafter "Chaum") in view of Boudot. Moreover, Claims 9 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Hopkins et al. (U.S. Patent Application No. 2003/0120931) (hereafter "Hopkins") in view of Boudot.

Applicants provide the following response and respectfully traverse rejections presented in the September 28, 2007 Final Office Action.

As a preliminary matter, Applicants have amended independent Claims 1, 5, 7, 9, 10, 12, 14, 16 and 18 to address the Examiner's Response to Arguments section beginning on page 2 of the office action- to specifically set forth an "exponent interval *I*" having a plurality of exponent elements, the interval having a specified first random limit. Respectfully, no new matter is being

added as full support for the limitation can be found in the originally disclosed specification, e.g., see discussion of the proof beginning on page 12, and more particularly, the discussion on page 13, lines 7 et seq. of the present specification that teaches an interval "*I*" being generated having more than some number of integers including so-called (l,v)-smooth integers.

Moreover, applicants amend each of Claims 1, 7, 10, 12, 14 and 18 to clarify that provided at a verifier, or second computing node, a public key comprising: an exponent-interval description having a specified first random limit and an interval width specification and, a public key value derived from a random secret key, said public key value including a random prime value, a number (n) corresponding to a product of two large prime numbers forming said secret key, an exponent interval *I* having a plurality of exponent elements, and two public values from a set of elements having a square root modulo n.

Respectfully, no new matter is being entered in these claims as full support can be found in the specification. For example, the public exponent-interval description (A,v) includes a specified first random limit (A) and an interval width specification (v) with definitions set forth in the Glossary found in the present application at pages 2 and 3. Further, the public key value derived from a random secret key includes values referred to in the specification as (n, h, x, e', and *I*) with e' being a random prime value, a number (n) corresponding to a product of two large prime numbers forming said secret key, an exponent interval *I* having a plurality of exponent elements, and two public values h, x from a set of elements having a square root modulo n.

According to one aspect of the invention, as claimed (E.g. Claims 10 and 18) using this public key value and exponent-interval description, one can easily verify whether the signature value from a first computer node is invalid if the selected exponent value is not contained in the exponent interval *I*.

Notwithstanding these limitations added to independent Claims 1, 5, 7, 9, 10, 12, 14, 16 and 18, the Examiner still rejects at least independent Claims 1, 12 and 14 as unpatentable based on Brennan in view of Arditti.

With regards to obviousness rejections of Claims 1-4, 12 and 14 as allegedly being unpatentable over Brennan in view of Arditti, and the obviousness rejections of Claims 5, 16 as allegedly being unpatentable over Brennan in view of Boudot, applicants respectfully disagree.

With respect to amended independent Claims 1, 12 and 14, nowhere in Brennan's disclosure does it mention that each element of the plurality of exponent elements of the exponent interval has a unique prime factor. Moreover, Brennan does not teach or suggest providing, at a verifier entity (a second computing node), a public key comprising: an exponent-interval description (A,v)having a specified first random limit and an interval width specification and, a public key value (n, h, x, *e'*, and *I*) derived from a random secret key, said public key value including a random prime value, a number (n) corresponding to a product of two large prime numbers forming said secret key, an exponent interval *I* having a plurality of exponent elements, and two public values from a set of elements having a square root modulo n

Brennan discloses a cryptographic key generation and safekeeping process whereby source code is loaded on a secure computer system with a "master-key" and "locking-key" compiled from the source code and then stored on disks (Abstract, Col. 12, lines 43-46). Moreover, Brennan describes a "public exponent e" which is derived from an RSA modulus N and private exponent d. (Col. 9, lines 19-28). However, Brennan is actually silent and fails to suggest or teach generating an exponent interval having a first random limit . . . each element of the plurality of exponent elements in the exponent interval having a unique prime factor as recited in the amended Claim 1. This notwithstanding, the Examiner also relies on the Brennan

specification at Col. 4, lines 53-60 teaching a plurality of unique key agents. Applicants fail to see how this passage in Brennan provides a teaching of an exponent interval having a first random limit . . . each element of the plurality of exponent elements in the exponent interval having a unique prime factor. The Brennan passage cited by the Examiner merely speaks to encrypting private key shares for shareholders designated as locking key agents in a particular public key system. Applicants respectfully fail to see how this is relevant to the Claims 1, 12 and 14.

Moreover, Brennan is primarily concerned with construction of master and lock keys for use within an organization to ensure their safekeeping. Nowhere in Brennan is their a specification of a public key having an exponent-interval description (A,v)having a specified first random limit and an interval width specification and, a public key value (n, h, x, e', and I) derived from a random secret key. In fact no definition of a public key suitable for use with Brennan's master and lock key system is disclosed.

Arditti, respectfully, is of no help in this regard either, as Arditti fails to suggest or teach the methods of Claims 1, 12 and 14 that includes (in part) a step of generating an exponent interval having a plurality of exponent elements, said interval an exponent interval having a first random limit . . . each element of the plurality of exponent elements in the exponent interval having a unique prime factor. Additionally, Arditti does not teach nor describe implementation of a public key having an exponent-interval description (A,v)having a specified first random limit and an interval width specification and, a public key value (n, h, x, e', and I) derived from a random secret key in the manner as now claimed in amended Claims 1, 7, 10, 12, 14 and 18.

While Arditti speaks to determining some sort of interval based on a parameter "m" from which an exponent value "α" that a "claimant" entity can use and an exponent "β" that a separate

"verifier" entity can use when applying hash functions according a special type of technique (called Diffie Hellman algorithm), this algorithm actually involves the generation of key values by both participants (a "claimant" as shown implementing steps Aa- Ad, Ca-Ce and "verifier" as shown implementing steps Ba-Bf in the paragraph bridging columns 4 and 5 of Arditti) in a manner that is completely different than the cryptographic technique implemented by claimant and verifier entities according to the present invention. In fact, Arditti places restrictions on the value of parameter "m" defining the "exponent interval" on col., 5, lines 36-41 that "m" may be equal to "n" (an integer of "adequate" size (see Arditti at col. 4, line 37) or on the same order as "k" but that is all that is said about the value of "m" much less the properties of the exponent elements in the exponent interval.

Thus, respectfully, Brennan, whether taken alone or in combination with Arditti which is directed to a completely different type of cryptographic system employing Diffie Hellman algorithm, and which is not compatible with the system of Brennan as demonstrated hereinabove, does not anticipate nor render unpatentable, at least of independent Claims 1, 12 and 14 as amended. Applicants respectfully request withdrawal of this rejection.

Applicants also note that the Office Action fails to appreciate the present invention, as recited in Claims 5 and 16, is further patentable over the combination of Brennan and Boudot as applied by the Examiner. That is, in view of the amendments to both claims 5 and 16, neither Brennan (as discussed hereinabove), nor Boudot teach a step of deriving the signature value from the following: a provided secret key, the selected exponent value from said plurality of exponent elements in said exponent interval, and the message, the signature value being sendable within the network to a second computer node for verification, wherein the each of said plurality of

exponent elements of the exponent interval has, with a probability close to certainty, a unique prime factor that is larger than a given security parameter.

Respectfully, while Boudot provides mathematical proof that a "committed" number can lie in an interval, there is no specific teaching in Boudot of implementation in an RSA-type encryption scheme such as employed in the Brennan. That is, the Examiner has relied upon Boudot, specifically, the teachings of section 4 (page 10 of the present office action), as teaching a method of publicly verifiable encryption scheme that proves that the value of an exponent lies in a specific interval. Applicants submit that the Boudot teaching found in section 4 is only an example application applied only to a specific kind of verifiable encryption scheme (Okamoto-Uchiyama cryptosystem) and has not proved that the Boudot's "proof" is extended to generating a signature that is verifiable by providing a public key having an exponent interval *I* having a plurality of exponent elements , wherein each element of said plurality of exponent elements of the exponent interval *I* has, with a probability close to certainty, a unique prime factor that is larger than a given security parameter; and, wherein a signature value is derived from a provided secret key, the selected exponent value from the plurality of exponent elements in said exponent interval, and the message, the signature value being sendable within the network to a second computer node for verification. includes a plurality of exponent elements. Without these teachings, Boudot in combination with Brennan, can not render Claims 5 and 16 unpatentable.

Applicants also note that the Office Action fails to appreciate the present invention, as recited in Claims 7-8, 10 and 18, is further patentable over the combination of Chaum and Boudot as applied by the Examiner.

With regards to the obviousness rejections of Claims 7-8, 10, 17-18, 20 as allegedly being unpatentable over Chaum in view of Boudot, with respect to Claims 7, 10 and 18, as

amended, neither Chaum nor Boudot teaches receiving, at a second computer node, a signature value, and, providing, at the second computer node, a public key comprising: an exponent-interval description having a specified first random limit and an interval width specification and, a public key value derived from the random secret key, said public key value including a random prime value, a number (n) corresponding to a product of two large prime numbers forming said secret key, an exponent interval *I* having a plurality of exponent elements, and two public values from a set of elements having a square root modulo n; and verifying, using said provided public key value, whether an exponent value is contained in an exponent interval *I* having a plurality of exponent elements, wherein each element of said plurality of exponent elements of the exponent interval has, with a probability close to certainty, a unique prime factor that is larger than a given security parameter, the signature value being invalid if the exponent value is not contained in the exponent interval.

In contrast, Chaum discloses that "at least one prime factor" is uniquely determined by the message. That is, the exponent referred to in the passage cited by the Examiner at col. 20, lines 30-43 of Chaum, is derived from the message by the first party (claimant) using a procedure known to first and second parties. In other words, Chaum fails to suggest or teach verifying whether an exponent value is contained in an exponent interval having a plurality of exponent elements, wherein each element of the exponent interval has, with a probability close to certainty, a unique prime factor that is larger than a given security parameter.

Boudot fails to remedy Chaum's deficiency as it merely provides an abstract proof related to "membership to an interval" and doesn't teach or suggest that each element of the exponent interval having a unique prime factor that is larger than a given security parameter as recited in Claim 7, 10 and 18.

Therefore, since both Chaum and Boudot fail to suggest or teach at least two features set forth in Claims 7, 10 and 18, they both fail to make obvious the present invention as recited in those claims.

Thus, in view of the foregoing amendments and remarks, the Examiner is respectfully requested to withdraw the rejections of independent Claims 1, 5, 7, 9, 10, 12, 14, 16 and 18 under 35 U.S.C. 103(a).

In view of the foregoing, this application is now believed to be in condition for allowance, and a Notice of Allowance is respectfully requested. If the Examiner believes a telephone conference might expedite prosecution of this case, it is respectfully requested that he call applicant's attorney at (516) 742-4343.

Respectfully Submitted,

Steven Fischman
Registration No. 34,594

Scully, Scott, Murphy & Presser, P.C.
400 Garden City Plaza, Suite 300
Garden City, New York 11530
(516) 742-4343

SF:gc